Maîtriser la sécurité du Système d'Information (SI)

Dr OUEDRAOGO Boukary

MD,MPH,PhD

OUEDRAOGO Ousséni
MDc,DU,MPH,Msc Candidate

Mail : ousseni.ouedraogo99@gmail.com

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Une démarche de sécurité du système d'Information (SI) dans un établissement ne peut exister sans l'impulsion de la direction pour légitimer sa mise en œuvre.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1 - LES OBJECTIFS DE LA SECURITÉ DU SYSTÈME D'INFORMATION (SI)

Trois grands objectifs sont fixés à la démarche de sécurité du SI.

1.1 - Objectif 1 : Garantir l'intégrité de l'information en évitant toute altération ou perte de données

Réduire le risque de perte ou d'altération des données du SI est l'un des objectifs principaux.

Questions

- Comment peut on limiter l’impact de cette perte de données du SI ?

- Comment rendre plus efficace votre méthode proposée ?

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Pour atteindre cet objectif, l'une des actions prioritaires doit porter sur **la mise en œuvre d'un plan de sauvegarde des données du SI.** L'expérience montre que ce plan n'est jamais efficace à moins d'être testé régulièrement (sauvegardes incomplètes, restauration impossible, absence de procédures de reprise des données non sauvegardées, etc.) ; ces tests sont **exécutés avec la collaboration des utilisateurs du SI** de l'établissement.

IMaîtriser la sécurité du Système d'Information (SI) – Comment ?

Pour garantir la qualité de l'information, les praticiens des établissements interrogés expriment le besoin de pouvoir **établir les responsabilités en cas d'anomalie ou d'altération sur des données** de santé.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Pour répondre à ces besoins, une deuxième action consiste à **activer dans les applications du SI, autant que possible, des fonctions de génération de traces associée aux opérations réalisées sur les données**; les traces obtenues doivent être conservées au moins 3 mois (historique des mouvements) pour pouvoir être exploitées en cas de recherche de la cause d'une anomalie.

Un incident touchant l'intégrité des données, vécu dans un établissement de la région Nord Pas-de-Calais

« Un matin, nous avons découvert des anomalies dans certains numéros de sécurité sociale de notre base de patients. La remise en état des 40.000 dossiers a nécessité l'intervention de deux personnes à temps plein pendant une semaine.»

Question

- Comment seriez vous sûr que les activités de votre service continuera malgré une panne au sein de votre système ?

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1.2 - Objectif 2 : S'assurer de la continuité des services en cas de défaut grave de l'informatique

Elaborer un plan de continuité d'activité pour s'assurer qu'en toutes circonstances, les activités vitales de l'établissement ne seront pas arrêtées.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

En cas d'arrêt du SI, ce plan prévoit des **procédures palliatives qui devront être suivies par les utilisateurs**. Des cas ont montré qu'un arrêt pouvait entraîner, s'il n'est pas correctement géré, des pertes de chances pour des patients, une perte d'image et des pertes d'activité pour l'établissement.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Les situations suivantes ont été vécues dans des établissements: le logiciel ou le serveur hébergeant le DPI ne fonctionne plus ; l'alimentation électrique est coupée ; un pourcentage important des postes informatiques sont infectés par un virus et ne fonctionnent plus.

Tous admettent qu'une **préparation adaptée avant ces incidents** mettant en œuvre des moyens techniques, des procédures, de l'organisation, aurait permis d'éviter des situations parfois critiques.

Question

- Quelles sont les méthodes que vous proposez pour garantir la sécurité des données à caractère personnel ?

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

1.3 - Objectif 3 : Garantir la confidentialité des données à caractère personnel

Un établissement de santé traite des données à caractère personnel qualifiées de sensibles par la loi « informatique et libertés »

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Au-delà de la **contrainte règlementaire**, et à côté du **préjudice** potentiellement grave subi par les patients dont les données médicales ont été divulguées, force est de constater que ces incidents (la **diffusion massive de données médicales**) font de plus en plus souvent l'objet d'une médiatisation et atteignent alors l'image de l'établissement.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Aussi, l'établissement doit mettre en pratique toutes les **mesures nécessaires pour garantir la confidentialité des données. Ces mesures ne sont pas que seulement techniques.** Elles nécessitent, pour être efficaces, d'adapter des processus métiers et de faire adhérer les professionnels de santé à des pratiques réflexes.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

2 - METTRE EN PLACE UNE ORGANISATION LEGITIME, CAPABLE D'ANIMER LA DEMARCHE

Dans le cadre d'une démarche sécurité, il faut mettre en place, le plus rapidement possible, une organisation de sécurité, identifiant à minima :

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

- **Un responsable de la démarche sécurité** à la fois reconnu et disposant d'une connaissance transverse des activités de l'établissement. Il a besoin de maîtriser ses processus et son organisation. Le responsable qualité de l'établissement peut être la bonne personne pour cette mission. **Il agit en tant que maître d'ouvrage sécurité**.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

- **Un correspondant opérationnel de la sécurité** ayant une bonne connaissance de l'informatique de l'établissement et des aspects techniques de sécurité. Il a en charge de mettre en œuvre et de maintenir les mesures de sécurité pour ce qui relève de l'informatique.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Remarque **:** *le* ***responsable*** *de la démarche sécurité peut être le* ***correspondant opérationnel*** *sécurité. Dans ce cas, la personne doit réunir à la fois des compétences techniques informatiques, et des capacités à conduire des projets transverses dans un établissement.*

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

- **Une instance de pilotage** (dédiée ou non) se réunissant périodiquement et dans laquelle seront évoqués les risques et les mesures opérationnelles de sécurité. Cette instance doit réunir une représentation aussi complète que possible des services de l'établissement (DRH, Services Généraux, Informatique, services de soins, services logistiques)

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

3 - INITIER UNE DEMARCHE D'AMELIORATION CONTINUE

La démarche sécurité est un processus d'amélioration continue **à l'instar de la qualité des soins**. Il faut donc pérenniser la démarche, ce qui passe par :

- **L'organisation d'un état des lieux périodique** permettant de réaliser un nouveau diagnostic, d'identifier les écarts restant à combler et de réactualiser un plan d'actions prioritaires.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

- **La définition de paliers de réalisation** des actions pour une atteinte progressive des objectifs. Ces actions nécessitent bien entendu des moyens.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

4 - INFORMER ET SENSIBILISER

Les objectifs de sécurité prioritaires doivent être connus de tous et partagés. Chacun doit connaitre les risques existants, la finalité des contraintes mises en place, et les bénéfices attendus pour l'établissement et la pratique des soins.

Maîtriser la sécurité du Système d'Information (SI) – Comment ?

Il est aussi nécessaire d'initier un programme de sensibilisation à la sécurité de SI, puisque ce sont souvent les erreurs humaines des utilisateurs dans l'établissement qui sont à l'origine des incidents, du fait de la négligence ou de l'ignorance des risques.

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

1 - ETABLIR UN PRE-DIAGNOSTIC SANS ETRE EXPERT : LES 10 QUESTIONS A SE POSER

« Tout va bien. L'ensemble du système d'information fonctionne ». Cette affirmation revient souvent lorsque la question d'un budget sécurité est à arbitrer par la Direction au détriment d'autres budgets jugés plus essentiels pour l'établissement.

Voici une dizaine de questions simples qui permettent de faire rapidement un premier bilan sur la maturité de sécurité atteinte.

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

1) Est-il possible de savoir combien d'heures ou de jours au total, le système d'information a été indisponible cette année? Mesurez-vous et surveillez-vous cet indicateur ?
2) Existe-t-il une politique de sécurité qui reflète la situation existante (document à jour) ? Les éventuels écarts par rapport à l'existant, l'appréciation de leurs conséquences potentielles sont-ils connus de la Direction ?

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

3) Le nombre de comptes d'accès nominatifs aux applications informatiques déclarés dans l'annuaire du SI est-il supérieur au nombre de personnes physiques accédant au système d'information ? Avez-vous encore des comptes génériques pour l'accès au SI ?

4) Les droits d'accès au DPI permettent-ils de garantir que seules les personnes autorisées ont la possibilité de modifier des données ?

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

5) Des données vitales seraient-elles perdues en cas d'incendie ou d'inondation dans un local technique hébergeant des serveurs ? Le temps qu'il faudrait pour rétablir le système informatique est-il connu ?

6) Les procédures de restauration des sauvegardes de données ont-elles déjà été testées ?

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

7) Quelle est l'ancienneté des serveurs ? La maintenance est-elle assurée ? Les systèmes sur ces serveurs sont-ils très régulièrement mis à jour ?

8) Les données RH concernant les informations sur les personnels de l'établissement font-elles l'objet d'une protection particulière ?

Comment mettre en place la démarche ; à qui déléguer le rôle de responsable ?

9) Est-il possible que dans certaines circonstances, un visiteur puisse accéder sans difficulté à un poste de travail ?

10) Dans le cas où un dossier médical de l'un de vos personnels aurait été consulté de manière illégitime, le service informatique serait-il en mesure de fournir des éléments pour investiguer ?

ARBITRAGE GUIDÉ PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

- **Il n'est pas toujours nécessaire de disposer d'un budget important** pour améliorer significativement le niveau de sécurité de l'établissement.
- Il faut d'abord privilégier les actions qui répondent à, au moins deux, des qualités suivantes : les moins coûteuses, les plus courtes, les moins contraignantes pour les utilisateurs du SI, les plus bénéfiques « rentables ». Elles sont dites des actions « pépites ».

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.1 - Des actions de bon sens mais à accompagner

Les actions « pépites » sont souvent considérées comme des actions de bon sens ; mais elles peuvent apporter de nouvelles contraintes à l'utilisateur que celui-ci peut refuser.

Le choix de ces actions doit être confronté aux pratiques du terrain dans un esprit de compromis entre la contrainte et le bénéfice apporté.

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.2 - Quelques exemples de « pépites »

- Supprimer les étiquetages des locaux critiques pour éviter d'attirer l'attention de personnes mal intentionnées.

- Fermer à clé les salles hébergeant les serveurs informatiques.

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.2 - Quelques exemples de « pépites »

- Activer les écrans de veille et le verrouillage du poste à la sortie de la veille.
- Demander aux utilisateurs ou au support de premier niveau de faire

  remonter en un point unique les incidents opérationnels et de sécurité.

  Etablir des rapports périodiques sur les incidents.

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.2 - Quelques exemples de « pépites »

- Déplacer les cartouches de sauvegarde pour qu'elles ne soient plus au même endroit que le robot de sauvegarde.

- Définir des fiches de postes pour tout le personnel du service informatique, intégrant les rôles et obligations en matière de sécurité.

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.2 - Quelques exemples de « pépites »

- Interdire un usage non professionnel et abusif des ressources informatiques (exemple, téléchargement de musiques ou de films etc.).
- Communiquer périodiquement sur les règles de sécurité à respecter au quotidien et sur le guide d’usage des moyens informatiques.

ARBITRAGE GUIDE PAR LA NATURE DES ACTIONS : LES ACTIONS « PEPITES »

2.2 - Quelques exemples de « pépites »

- Remplacer les identifiants génériques des administrateurs par des identifiants nominatifs.
- Revoir les droits d'accès aux répertoires partagés contenant de l'information à caractère personnel.
- Formaliser les procédures d’intervention à distance sur l’informatique de l’établissement

La communication : un levier essentiel

Communiquer auprès des utilisateurs est une priorité, car les usages qu'ils font du système d'information sont à l'origine de la majorité des incidents de sécurité :

- ✓**Oublier un document sur une imprimante ;**
- ✓**Stocker des fichiers sans se préoccuper des sauvegardes ;**
- ✓**Installer des applications informatiques sans prévenir le responsable des Systèmes d'Information ;**

La communication : un levier essentiel

- ✓**Identifier des erreurs sans faire remonter l'information ;**
- ✓**Considérer que se préparer à faire face à un arrêt temporaire de l'informatique est une perte de temps ;**
- ✓**Utiliser une messagerie non sécurisée pour transmettre (hors de l'établissement) des informations médicales sur un patient.**

Tous ces exemples sont autant de comportements risqués qui peuvent être évités par une action adaptée et régulière d'information.

MERCI